ET4394
WIRELESS NETWORKING
Wireshark Assignment

March 6, 2018

Himanshu Shah (4739779)
Priyanka Bhat (4735153)

Objective

In this project, we have captured a large set of Access point(AP) data and performed lexical analysis on their SSID. To accomplish this task we used tshark, a network protocol analyzer which lets you capture data from a live network or read packets from a previously captured file, to capture live packets from the AP's in the surrounding and then used shell script to filter out data to metrics we require and then performed further lexical analysis on it.
The most important part of the project was to collect as much diverse data as possible. So, we collected data across different locations in campus, around the city and various student housing. After, collecting the data we analyzed the data and tried to figure out common patterns and stereotypes in the way people assign names for their SSID which has been illustrated in document further.

Technical Setup and Working

To begin with first we need to have t-shark working on the device to capture network packets. tshark can be installed using the below command:
`sudo apt-get install wireshark`
Note: We have used Linux system with Ubuntu 16.04 LTS distribution.

By default, if we capture packets over a network it does not contain information about SSID and only contains packets that are addressed to our system. In order to capture packets from other users we need to use `promiscuous mode` and we need to enable `monitor mode` so that packets contain SSID information in them. Since, we are just concerned with the SSID of different AP's, and as that data is included in the packets captured using monitor mode, we won't be using promiscuous mode for this project.

To enable capturing packets in linux, we need to install an additional tool named aircrack-ng. This tool allows you to enable monitoring mode on the interface that you want to listen to. The following command can be used to install the tool,
`sudo apt-get install aircrack-ng`

In order to start capturing packets, we need to first find the name of the interface that we want to capture packets on. To know the name of interface, we can use command `ifconfig`. There might be some processes that can interfere or affect packet capturing, so we should

determine these processes and kill them before starting capturing. The command to do so is listed below

```
airmon-ng check
airmon-ng check kill
```

Note: This might also kill your network manager. But, you can start it again later using `service start NetworkManager.`

Now, we can start monitor mode on our interface. To enable monitor mode, run the following command,

```
airmon-ng start <your-interface-name>
```

This will start monitor mode on the listed interface or create a new interface (usually mon0) for using monitor mode. To confirm if monitor mode has been enabled use command `iwconfig` and you should be able to see an interface with `Mode:Monitor`. Next, we can use tshark to start collecting packets. To start tshark following stated command can be used:

```
tshark -i <monitor-mode-interface> -I
```

The above command starts capturing packets on the listed interface. The flag `-I` indicates tshark to use monitor mode. In addition you can also specify duration for which you want to capture, output file types, size limit of file etc. We used a shell script to accomplish the tasks of starting airmon-ng, executing tshark and writing the output to a text file.

Observations

During the project, data was collected at various locations and we have categorized the observations into four categories: Housing, Campus, City and Collective. We observed average length of SSID's, most frequent word, number of hidden SSID's, number of SSID's with default name and the naming pattern people use for each of the categories. We have also provided the plots for each category which includes the percentage of the SSID's that contain abuses, special characters (excluding the most commonly used -, _ characters), names of food items, animals, acronyms and letters only.

Housing Category

For the housing category, we found 309 **Unique SSID's**. The **average length** of SSID's in this category turned out to be 11. **Words that appeared frequently** along with their frequency are Huize(5), Wifi(3), Router(3), 2.4Ghz(3), yo(2). The plot for housing category in shown in Figure 1.

City Category

For the city category, we found 768 **Unique SSID's**. The **average length**of the SSID's in this category turned out to be 11.**Words that appeared frequently** along with their frequency are Huize(8), Delft(8), De(7), 5G(5), &(3). The plot for city category in shown in Figure 2.

Campus Category

For the Campus category, we found 69 **Unique SSID's**. The **average length** of SSID's in this category turned out to be 10. **Words that appeared frequently** along with their frequency are Wifi(7),MAVSTART(4), Ziggo(2). The plot for campus category in shown in Figure 3.

Overall

Overall, all the categories combined, we found 1146 **Unique SSID's**. The **average length** of SSID's in this category turned out to be 11. **Words that appeared frequently** along with their frequency are: in(10), Ziggo(9), 5G(8), Huize(13), Delft(8). The plot for collective category in shown in Figure 4.

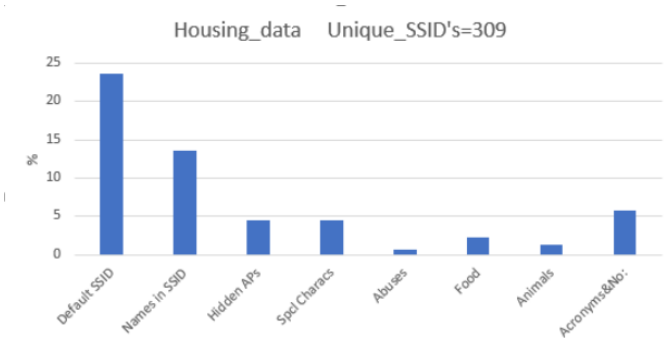

Figure 1: Plot for data across housing areas

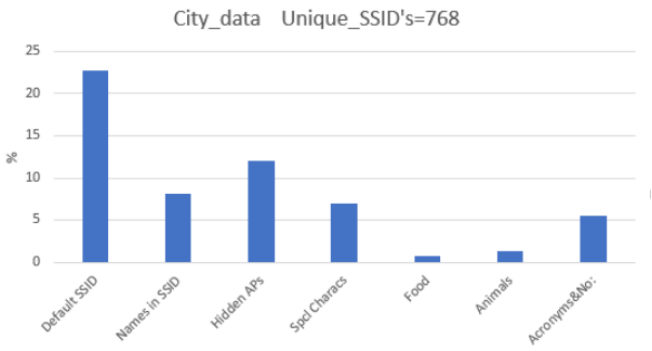

Figure 2: Plot for data across city areas

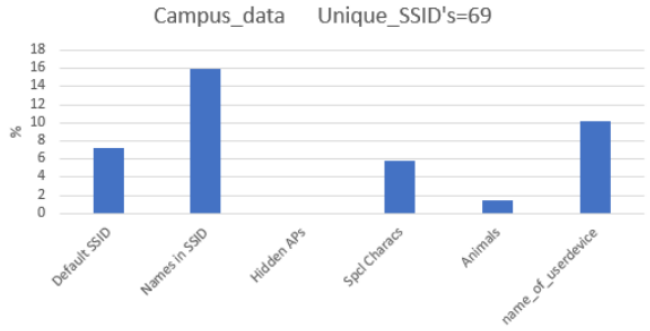

Figure 3: Plot for data across campus areas

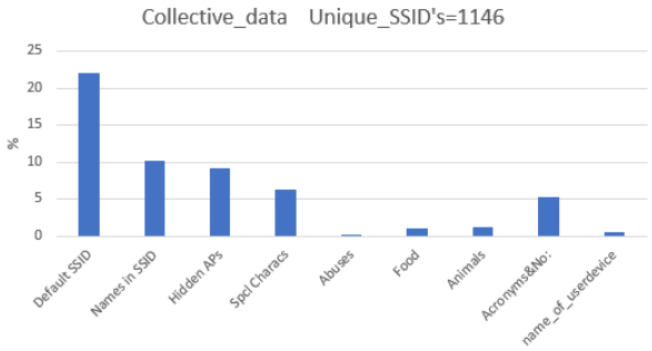

Figure 4: Plot of the collective data

The following category lists some of the SSID's that have a **funny/abusive** side to it. IPPwhenIPooPoo, 2 girls 1 router, MTBitches2, FuckTariq, Mom, click here for internet, IthurtswhenIP, Probleem?, love is in the air <3, Flowwjob, ModernDayCocaine, Hide yo kids hide yo wifi, No Need, Password is Pizza, We have your penguin.

Results

From project, we observed that about 22 percent of the people have SSID's that are default and do not change it and about 10 percent of the people use their brand, shop or own name as SSID. We also found hidden SSID which formed about 9 percent of the total share.